DEPLOYMENT GUIDE
Version 1.4

IMPORTANT: This guide has been archived. While the content in this guide is still valid for the products and version listed in the document, it is no longer being updated and may refer to F5 or 3rd party products or versions that have reached end-of-life or end-of-support. See https://support.f5.com/csp/article/K11163 for more information.

Configuring IP Address Sharing in a Large Scale Network: DNS64/NAT64

Configuring the BIG-IP LTM for the private IPv4 network

It is well-known that private IP addresses (defined per RFC1918) have been used by most enterprises, some small service providers and mobile operators. The same private space could also be used to help overcome global IPv4 depletion.

In this scenario, the BIG-IP LTM acts as a gateway device that translates clients' private addresses to a set of global IPv4 addresses. This requires a wildcard forwarding virtual server with SNAT pool on the BIG-IP LTM.

Creating the SNAT Pool

In this procedure, we configure a SNAT pool. A secure network address translation (SNAT) translates the source IP address within a connection to a BIG-IP system IP address that you define. A SNAT pool is a group of these IP addresses.

Popular websites with heavy traffic (such as Google and Facebook) may require more SNAT addresses than typical websites. To estimate number of SNAT address you need for these high-traffic sites, you must have a number of SNAT addresses larger than the maximum number of concurrent connections per destination IP address divided by 64,000 (Number of SNAT address > (maximum concurrent connections per destination IP address / 64,000)).

For example, if the destination IP address has 250,000 maximum concurrent connections, you would need **4** SNAT addresses in the SNAT pool (250,000/64,000 = 3.906). You want to make sure you have enough SNAT addresses to cover the site with the highest expected traffic.

◆ Tip

It is outside the scope of this document to show you how to determine the number of concurrent connections, we recommend you use an appropriate monitoring tool. You could also use the BIG-IP LTM to determine concurrent connections by creating a virtual server that has a destination that matches the website you want to monitor. Then view the virtual server statistics to view the number of connections.
*Another indicator is if any of the log messages in **/var/log/ltm** mention port exhaustion.*
For more information, see the BIG-IP LTM documentation.

For more information on SNAT pools, see the *Configuring SNATs* chapter in the **Configuration Guide for Local Traffic Management**.

To create the SNAT pool

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. On the Menu Bar, click **SNAT Pool List**.

3. Click the **Create** button.
4. In the **Name** box, type a name for this SNAT pool. In our example, we type **LSN-snat-pool**.
5. In the **IP Address** box, type an otherwise unused IP address, and click the **Add** button.

   Repeat this step for each additional address needed, from your calculation above.
6. Click **Finished**.

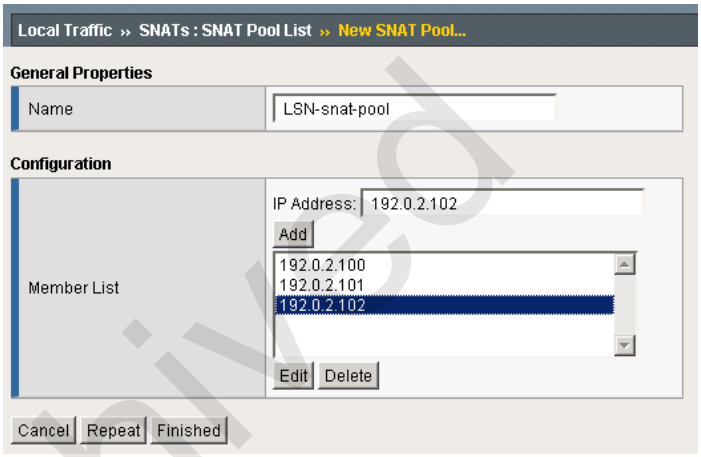

Figure 1 *SNAT pool configuration*

Using an iRule to choose a SNAT address (optional)

You can optionally define an iRule on the BIG-IP system that selects a specific SNAT address. By default, the BIG-IP LTM picks address from the SNAT pool in a round-robin fashion. Some applications or websites may use multiple connections (or even multiple destinations) per session, and the application may break if the client accesses from a different source IP. The following simple iRule can be used to ensure client always uses the same SNAT address.

This iRule picks a SNAT address related to the last octet of the client IP address. For example, if the client address is 172.16.33.57, the BIG-IP system uses the SNAT address 10.10.10.58 (notice the last octet is one higher). This simple example assumes there are 64 SNAT addresses from 10.10.10.1 through 10.10.10.64.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **snat-pool-irule**.

4. In the Definition section, copy and paste the following iRule:

```
1   when CLIENT_ACCEPTED {
2       snat 10.10.10.[expr ( [getfield [IP::client_addr] "." 4] % 64 ) + 1 ]
3   }
```

5. Click **Finished**.

Note

This SNAT iRule overwrites the SNAT setting from the virtual server.

Creating the wildcard virtual server

The next task it to configure a wildcard virtual server that contains the SNAT pool you created.

By default, this wildcard virtual server is enabled on all VLANs. As an optional step for added security, you can lock down the virtual server to specific VLANs in step 11.

To create the wildcard virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **LSN_wildcard**.
4. In the Destination row, click the **Network** option button.
5. In the **Address** box, type **0.0.0.0**.
6. In the **Mask** box, type **0.0.0.0**.
7. In the **Service Port** box, type ***** or select ***All Ports** from the list.
8. From the **Configuration** list, select **Advanced**.
9. From the **Type** list, select **Forwarding (IP)**.
10. From the **Protocol** list, select ***All Protocols**.
11. *Optional*: From the **VLAN and Tunnel Traffic** (or **VLAN Traffic** in some versions) list, select **Enabled on**.
    From the Available list, select the appropriate VLANs and then click the Add (<<) button.
12. From the **SNAT Pool** list, select the SNAT Pool you created in *Creating the SNAT Pool*. In our example, we select **lns-snat-pool**.

13. *Optional*: If you created the iRule in *Using an iRule to choose a SNAT address (optional)*, in the Resources section, from the **iRule Available** list, select the iRule you created and click the Add (<<) button.
14. Click **Finished**.

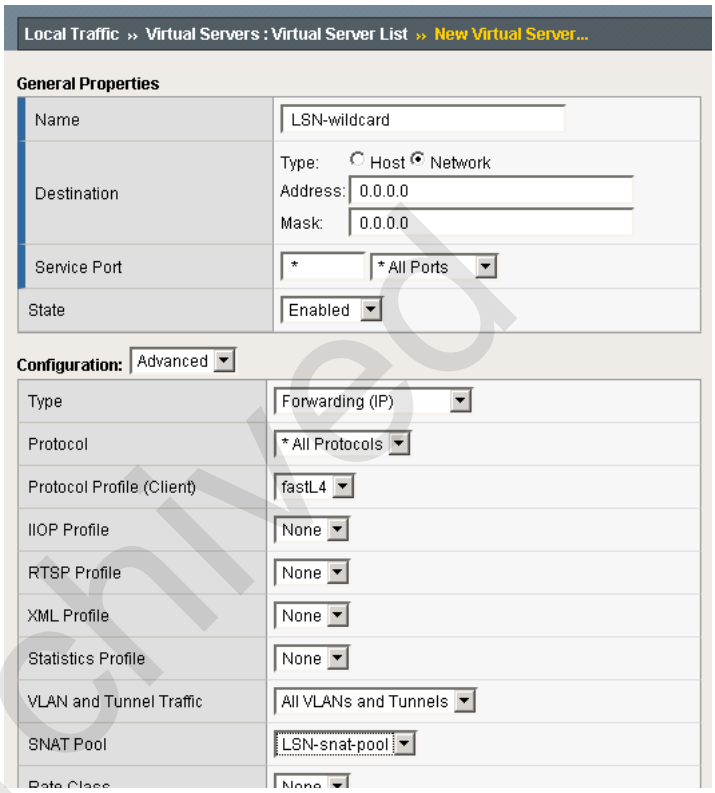

Figure 2 *Wildcard virtual server configuration (truncated)*

Note

Because this is a forwarding virtual server, the BIG-IP system forwards traffic based on routing. You may need to configure a default gateway on the BIG-IP LTM. See the online help or BIG-IP documentation for more information.

Supporting NAT with active FTP mode (optional)

To support active mode FTP traffic from clients, you need to configure an additional wildcard virtual server and apply an FTP profile to it. We create this virtual server so the BIG-IP system can detect the ephemeral data port which the client opens, and rewrite it to the SNAT address/available

ephemeral port. The BIG-IP system also listens on the address/port (that it rewrites) and translates it to the actual address/port to which the client is listening.

The first task in this section is to create a FTP profile.

To create the FTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Services** menu, click **FTP**.
3. Click the **Create** button.
4. In the **Name** box, type a name. In our example, we type **LSN-ftp**.
5. Configure any of the settings as applicable for your configuration. In our example, we leave the defaults.
6. Click **Finished**.

Next we create the virtual server.

To create the wildcard virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **FTP_wildcard**.
4. In the Destination row, click the **Network** option button.
5. In the **Address** box, type **0.0.0.0**.
6. In the **Mask** box, type **0.0.0.0**.
7. In the **Service Port** box, type **21** or select **FTP** from the list.
8. Leave the **Type** list set to **Standard**.
9. From the **FTP Profile** list, select profile you created in the preceding procedure. In our example, we select **LSN-ftp**.
10. *Optional*: From the **VLAN and Tunnel Traffic** (or **VLAN Traffic** in some versions) list, select **Enabled on**.
    From the Available list, select the appropriate VLANs and then click the Add (<<) button.
11. From the **SNAT Pool** list, select the SNAT Pool you created in *Creating the SNAT Pool*. In our example, we select **LNS-snat-pool**.
12. Click **Finished**.

This concludes the BIG-IP LTM configuration for the private IPv4 network.